한국컴퓨터정보학회 동계학술대회 논문집 제26권 제1호 (2018. 1)

이더리움을 이용한 에스크로 서비스 개선 모델

정한재O
O숭실대학교 소프트웨어특성화대학원
e-mail: yongumi@gmail.comO

An Improvement Model of Escrow Service Using Ethereum

Han-jae JeongO
ODept. of Software, Soong-Sil University Graduate School

● 요 약 ●

에스크로는 개인 간의 물품 거래를 중개하여 허위 물품 등록 및 대금 횡령과 같은 사기를 방지하는 안전 결제 서비스이다. 그러나 신뢰할 수 없는 에스크로 서비스 사로 인한 사기 발생 및 에스크로의 서비스 구조와 같은 태생적인 한계로 인한 이용률 저하와 같은 한계점들은 건전한 사용자들의 이용률을 저하시킨다. 본 논문에서는 이런 문제점들을 극복하기 위해 블록체인 플랫폼 중 하나인 이더리움을 이용하여 개선된 에스크로 서비스 모델을 제시하고자 한다.

키워드: 에스크로, 블록체인, 이더리움

I. Introduction

'에스크로'란 개인 간 상거래에서 신뢰할 수 있는 제3자에게 물품 및 대금을 맡겨두었다가 구매자 및 판매자 양측의 승인을 통해 거래가 이루어지는, 안전한 거래를 도와주는 서비스를 의미한다. 하지만 신의성실의 원칙을 위배하는 에스크로 서비스 기업, 서비스 자체의 태생적인 한계로 인한 낮은 경제적 실효성과 같은 단점들은 취지에 비해 사용자들의 이용률을 낮추고 약속 불이행과 같은 부작용을 낳기도 한다. 본 논문에서는 블록체인 플랫폼의 하나인 이더리움을 활용하여 이러한 한계들을 극복하는 새로운 모델을 제시하고자 한다.

II. Preliminaries

1. 기존 에스크로 서비스의 문제점

1.1 신뢰할 수 없는 에스크로 서비스 제공자

대금을 보관하는 에스크로 서비스 제공자가 의무를 제대로 이행하지 않음으로써 생기는 약속 불이행 문제는 매년 끊임없이 발생하고 있다.[1] 이를 보완하기 위해 에스크로 업체의 자격요건 및 제도적 보완책 등을 제정하였으나 이는 근본적인 해결책이 되지 못한다.

1.2 높은 수수료로 인한 이용률 저하

물품의 가치에 따라 상대적인 것이 아닌 고정된 수수료 및 높은 최소 수수료의 책정은 저렴한 가격의 물품의 거래의 경우 에스크로 서비스를 사용하기 힘든 부분이 있다. 또한 다른 국가 사용자들간의 거래의 경우 통화를 일치시키기 위해 페이팔(Paypal)과 같은 중재자가 추가로 필요하여 수수료가 높아지는 문제가 존재한다.

2. 블록체인

2008년 <비트코인:개인 간 전자화폐 시스템>이라는 백서에서 블록과 체인이라는 표현으로 처음 등장한 자료구조이자 분산 데이터베이스로, 모든 블록의 해쉬 값들이 리스트처럼 연결되어 있다. 블록체인을 기반으로 한 가장 처음 등장한 구현체인 비트코인은 운영주체가 없이 미리 정해진 비트코인 프로토콜 대로 동작하며 중앙 서버가 존재하지 않는다. 또한 모든 구현체 및 블록 정보는 공개되어 있으며, 모든 비트코인 네트워크 사용자들은 통일된 전자화폐를 사용한다.

3. 이더리움

비트코인 프로토콜을 기반으로 만들어진 새로운 블록체인 프로토콜이자 플랫폼이다. 트랜잭션 영역에 거래 장부를 기록하는 비트코인과는 달리 바이트 코드(Byte Code)를 기록하며, 그 코드를 EVM(Ethereum Virtual Machine)을 통해 해석하고 실행한다. 이러한 코드를 스마트 컨트랙트(Smart Contract)라 한다.[2]

III. The Proposed Scheme

1. 이더리움을 이용한 개선 모델

본 논문에서 제시하는 이더리움 기반 에스크로 서비스 개선 모델은 다음 Fig.1과 같다.

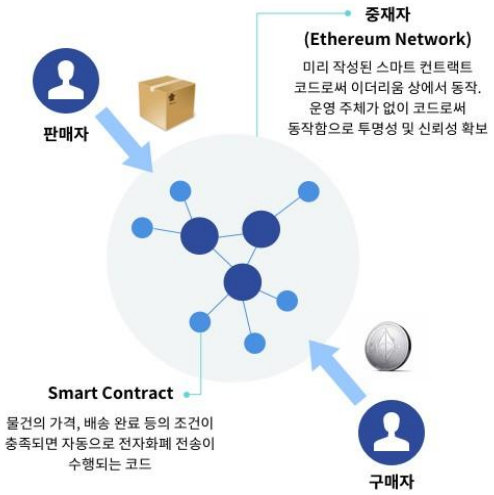

Fig. 1. 이더리움 기반 에스크로 서비스 모델

판매자가 작성한 판매의 조건 및 구매자가 그 조건에 동의하여 발생한 송금의 이행과 같은 모든 동작은'스마트 컨트랙트' 라 불리는 코드대로 수행됨으로써 판매자 및 구매자 모두 정해진 계약을 이행하도록 한다. 이때 화폐는 이더리움 전자화폐를 이용함으로써 추가적인 환전없이 스마트 컨트랙트를 수행하는데 필요한 최소한의 화폐만 사용하도록 한다.

2. 개선된 모델의 기대 효과

위와 같은 이더리움을 이용하여 구현한 에스크로 개선 모델은 중앙 서버 및 운영 주체가 없어 스마트 컨트랙트를 이용하는데 필요한 최소한의 수수료로 서비스 운영이 가능하다. 또한 이더리움 블록체인 네트워크는 단일 지점이 존재하지 않아 서비스 집중 공격 으로부터 안전하며, 네트워크 내 과반수 이상의 동의를 구하여야 데이터 변경이 가능하다는 점은 데이터 위변조 공격으로부터 안전성을 확보할 수 있다. 또한 모든 거래 기록이 남고 공개되어 투명한 운영이 가능한 점과 같은 특징이 있다.

IV. Conclusions

기존의 에스크로 서비스 업체가 담당하는 중재자 부분을 운영주체가 없는 P2P 네트워크 노드에서 동작하는, 위변조가 불가한 프로그램 코드로 변경하였다. 이는 공신력 없는 업체로 인한 신뢰성 하락 및 소액 거래에 대한 수수료 부담과 같은 문제 등을 해결할 수 있을 것이라 기대한다. 또한 모든 구현체는 공개되어 공익성을 띔으로써, 기존의 공신력 있는 업체에 에스크로 사업을 맡기려던 노력에 기술적인 일조를 할 수 있으리라 생각한다.

REFERENCES

[1] Soonduck Yoo, Kwangdon Choi, "Consumer protection in e-commerce: the Safety Transaction Service in Korea", Journal of Digital Convergence, vol.11 No.11, pp.29-36, 2013.

[2] Jeong Ho Suh, Taiki Lee, Gongpil Choi, "Policy Issues and application cases of Blockchain in the financial services industry", KIF financial report, No.2, 2017.